Результаты теста антивирусов на лечение активного заражения (Тест №1 от 02.2007)

http://www.anti-malware.ru/

Таблица 1: Результаты лечения активного заражения различными антивирусными продуктами

Антивирус \ вредоносное ПО	Adware.Win32.Look2me	Adware.Win32.NewDotNet	Backdoor.Win32.Haxdoor	Trojan-Proxy.Win32.Xorpix	Email-Worm.Win32.Scano	Email-Worm.Win32.Bagle	Trojan-PSW.Win32.LdPinch	Worm.Win32.Feebs	Trojan-Clicker.Win32.Costrat	Trojan-Spy.Win32.Goldun
Avast! Professional Edition 4.7	+	+	-	-	-	+	+	-	-	+
AVG Anti-Virus PE 7.5	-	+	-	-	-	+	+	-	-	+
Avira AntiVir CE 7.0	-	-	-	-	-	+	+	+	-	-
AVZ 4.21	-	+	+	-	-	+	+	-	+	-
BitDefender Antivirus 10	-	+	+	-	-	+	+	+	-	-
Dr.Web Anti-Virus 4.33	-	-	+	-	-	+	+	-	-	-
Eset NOD32 Antivirus 2.7	-	-	+	-	-	+	+	+	-	+
F-Secure Anti-Virus 2007	-	-	-	-	-	+	+	+	-	-
Kaspersky Anti-Virus 6.0	+	+	+	+	+	+	+	-	-	-
McAfee VirusScan 2007	-	+	-	-	-	+	+	+	-	-
Panda Antivirus 2007	+	-	+	-	-	+	+	-	-	-
Sophos Anti-Virus 6.0	-	+	-	-	-	+	+	+	-	+
-	+	+	-	+	-	+	+	+	+	+
Trend Micro PC-Cillin 2007	-	+	-	-	-	+	+	-	-	-
VBA32 Antivirus 3.11	-	-	-	-	-	+	+	+	-	-

\+ - антивирус успешно устранил активное заражение, работоспособность системы восстановлена (не нарушена).

\- - антивирус не смог устранить активное заражение или была серьезно нарушена работоспособность системы.

Таблица 2: Итоговые результаты лечения

Антивирус	Всего вылечено	Позиция
Norton AntiVirus 2007	**8**	**1-е место**
Kaspersky Anti-Virus 6.0	**7**	**2-е место**
Avast! Professional Edition 4.7	**5**	**3-е место**
Eset NOD32 Antivirus 2.7		
Sophos Anti-Virus 6.0		
BitDefender Antivirus 10		
AVZ 4.21		
AVG Anti-Virus PE 7.5	**4**	
McAfee VirusScan 2007		
Panda Antivirus 2007		
Avira AntiVir CE 7.0	**3**	
Dr.Web Anti-Virus 4.33		
F-Secure Anti-Virus 2007		
Trend Micro PC-Cillin 2007		
VBA32 Antivirus 3.11		

Подробные результаты лечения по каждому вирусу смотрите по ссылкам ниже:

Антивирус	Вердикт	Adware.Win32.Look2me
Avast! Professional Edition 4.7	+	Во время плановой перезагрузки удалил все зараженные dll
AVG Anti-Virus PE 7.5	-	Детектирует только родительский файл.
Avira AntiVir CE 7.0	-	Не может проверить зараженные dll, выводится предупреждение "The file could not be opened!"
AVZ 4.21	-	Детектирует прямое чтение из памяти dll-компонент, но не предлагает их удалить.
BitDefender Antivirus 10	-	Успешно детектирует только одну из dll-компоненту, но заражение не ликвидируется.
Dr.Web Anti-Virus 4.33	-	После установки антивируса и перезагрузки выводится ошибка winlogon.exe и исчезает рабочий стол.
Eset NOD32 Antivirus 2.7	-	Успешно детектирует заразу, но при попытке удаления файл с именем вида zam0931e.dll появляется вновь после перезагрузки.
F-Secure Anti-Virus 2007	-	- Не может удалить dll--компоненту, после удаления/карантина файлы появляются под новыми именами, с guard.tmp не удается совершить никакие действия.
Kaspersky Anti-Virus 6.0	+	Успешно обнаружены и удалены все dll-компоненты и guard.tmp в папке %System%.
McAfee VirusScan 2007	-	Детктировал и удалил только %System%\guard.tmp
Panda Antivirus 2007	+	Успешно обнаружены и удалены все dll-компоненты в папке %System%.
Sophos Anti-Virus 6.0	-	При проверке зараженных dll выдается ошибка SAV Interface Error, file could not be accessed.
Symantec Norton AntiVirus 2007	+	Вредоносная программа была детектирована после установки и полностью удалена после перезагрузки
Trend Micro PC-Cillin 2007	-	Детектируется только родительский файл.
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	Adware.Win32.NewDotNet
Avast! Professional Edition 4.7	+	Остались следы пребывания Adware в системе: выводится ошибка при старте ОС, исчез доступ в Интернет.
AVG Anti-Virus PE 7.5	+	Остались следы пребывания Adware: исчез Интернет.
Avira AntiVir CE 7.0	-	Не может удалить файл залоченный newdotnet6_38.dll (в том числе после перезагрузки ОС).
AVZ 4.21	+	Остались следы пребывания Adware в системе: выводится ошибка при старте ОС, исчез доступ в Интернет.
BitDefender Antivirus 10	+	Остались следы пребывания Adware в системе: исчез доступ в Интернет.
Dr.Web Anti-Virus 4.33	-	Ошибка при попытке удаления файла newdotnet6_38.dll после перезагрузки, Spyder Guard не запускается.
Eset NOD32 Antivirus 2.7	-	Детектируется только родительский файл.
F-Secure Anti-Virus 2007	-	Не может удалить залоченный файл newdotnet6_38.dll, пропал доступ в Интернет.
Kaspersky Anti-Virus 6.0	+	Остались следы пребывания Adware в системе: выводится ошибка при старте ОС
McAfee VirusScan 2007	+	
Panda Antivirus 2007	-	Не может удалить залоченный файл newdotnet6_38.dll, который после "уничтожения" появляется вновь и вновь.
Sophos Anti-Virus 6.0	+	
Symantec Norton AntiVirus 2007	+	
Trend Micro PC-Cillin 2007	+	
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	Backdoor.Win32.Haxdoor
Avast! Professional Edition 4.7	-	Детектируется только родительский файл.
AVG Anti-Virus PE 7.5	-	Детектируется только родительский файл.
Avira AntiVir CE 7.0	-	Находит залоченный файл svkvpn.dll, с которым ничего не может сделать, не детектирует родительский упакованный файл.
AVZ 4.21	+	Удалены файлы svjvpn.sys и svkvpn.dll в папке %system32% при перезугрузке, остальные не детектирует.
BitDefender Antivirus 10	+	Удалены файлы svkvpn.dll и go.sys в папке %system32%, остальные не детектирует.
Dr.Web Anti-Virus 4.33	+	Удалены файлы svkvpn.dll, go.dll, go.sys, svjvpn.sys, svkvpn.sys в папке %system32% (за два прохода с перезагрузками).
Eset NOD32 Antivirus 2.7	+	Удалены файлы svkvpn.dll, go.dll, go.sys, svjvpn.sys, svkvpn.sys из папки %system32% и C:\WINDOWS\Temp\INF14.tmp за один проход.
F-Secure Anti-Virus 2007	-	Удалены только файл svkvpn.dll в папке %system32% при перезугрузке.
Kaspersky Anti-Virus 6.0	+	Удалены файлы svkvpn.dll, go.dll, go.sys, svjvpn.sys, svkvpn.sys в папке %system32% (за два прохода с перезагрузками).
McAfee VirusScan 2007	-	Невозможно установить антивирус.
Panda Antivirus 2007	+	Удалены файлы svkvpn.dll, go.dll, go.sys, svjvpn.sys, svkvpn.sys в папке %system32% (за два прохода с перезагрузками).
Sophos Anti-Virus 6.0	-	Удалены только файл svkvpn.dll в папке %system32%
Symantec Norton AntiVirus 2007	-	BSOD при первой перезагрузке после установки антивируса.
Trend Micro PC-Cillin 2007	-	Детектирует только svkvpn.dll, удалить который автоматически не может, предлагает удалить его вручную.
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	TrojanProxy.Win32.Xorpix
Avast! Professional Edition 4.7	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
AVG Anti-Virus PE 7.5	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Avira AntiVir CE 7.0	-	C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll [WARNING] The file could not be opened!
AVZ 4.21	-	
BitDefender Antivirus 10	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Dr.Web Anti-Virus 4.33	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Eset NOD32 Antivirus 2.7	-	C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dllerror opening (File locked) [4]
F-Secure Anti-Virus 2007	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Kaspersky Anti-Virus 6.0	+	Успешно удален C:\DOCUMENTS AND SETTINGS\ALL USERS\Äîêóìåíòû\SETTINGS\ARM32.DLL//Upack
McAfee VirusScan 2007	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Panda Antivirus 2007	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Sophos Anti-Virus 6.0	-	Не видит инфицированный файл C:\Documents and Settings\All Users\Äîêóìåíòû\Settings\arm32.dll
Symantec Norton AntiVirus 2007	+	Обнаружен по записи в реестре, обезврежен после перезагрузки.
Trend Micro PC-Cillin 2007	-	Детектируется только родительский файл.
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	Email-Worm.Win32.Scano
Avast! Professional Edition 4.7	-	Успешно удаляет файл csrss.exe из папки %Windows%, но после перезагрузки исчезает рабочий стол.
AVG Anti-Virus PE 7.5	-	Успешно удаляет файл csrss.exe из папки %Windows%, но после перезагрузки исчезает рабочий стол.
Avira AntiVir CE 7.0	-	Обнаруживает, но не может удалить/переместить зараженный файл C:\Windows\csrss.exe, после попытки удаления/перемещения файл появляется вновь.
AVZ 4.21	-	Успешно удаляет файл csrss.exe из папки %Windows%, но после перезагрузки исчезает рабочий стол.
BitDefender Antivirus 10	-	Успешно удаляет файл csrss.exe из папки %Windows%, но после перезагрузки исчезает рабочий стол.
Dr.Web Anti-Virus 4.33	-	Обнаруживает, но не может удалить/переместить зараженный файл C:\Windows\csrss.exe, после попытки удаления/перемещения файл появляется вновь.
Eset NOD32 Antivirus 2.7	-	После перезагрузки успешно удаляет файл csrss.exe из папки %Windows%, но исчезает рабочий стол.
F-Secure Anti-Virus 2007	-	Обнаруживает, но не может удалить/переместить зараженный файл C:\Windows\csrss.exe, после попытки удаления/перемещения файл появляется вновь.
Kaspersky Anti-Virus 6.0	+	+ Успешно удален файл csrss.exe из папки %Windows%
McAfee VirusScan 2007	-	Успешно удаляет файл csrss.exe из папки %Windows%, но после перезагрузки исчезает рабочий стол.
Panda Antivirus 2007	-	Обнаруживает файл C:\Windows\csrss.exe и предлагает перезагрузиться, после чего при старте ОС машина всегда зависает.
Sophos Anti-Virus 6.0	-	После перезагрузки успешно удаляет файл csrss.exe из папки %Windows%, но исчезает рабочий стол.
Symantec Norton AntiVirus 2007	-	После перезагрузки успешно удаляет файл csrss.exe из папки %Windows%, но исчезает рабочий стол.
Trend Micro PC-Cillin 2007	-	Успешно удаляет файл csrss.exe из папки %Windows%, но после перезагрузки исчезает рабочий стол.
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	Email-Worm.Win32.Bagle
Avast! Professional Edition 4.7	+	Успешно удалены компоненты m_hook.sys и hidn.exe из %UserProfile%\Application Data\hidn\
AVG Anti-Virus PE 7.5	+	
Avira AntiVir CE 7.0	+	
AVZ 4.21	+	
BitDefender Antivirus 10	+	
Dr.Web Anti-Virus 4.33	+	
Eset NOD32 Antivirus 2.7	+	
F-Secure Anti-Virus 2007	+	
Kaspersky Anti-Virus 6.0	+	
McAfee VirusScan 2007	+	
Panda Antivirus 2007	+	
Sophos Anti-Virus 6.0	+	
Symantec Norton AntiVirus 2007	+	
Trend Micro PC-Cillin 2007	+	
VBA32 Antivirus 3.11	-	

Антивирус	Вердикт	Trojan-PSW.Win32.LdPinch
Avast! Professional Edition 4.7	+	Удален при первой перезагрузке C:\WINDOWS\csrss.exe
AVG Anti-Virus PE 7.5	+	При перезагрузке удален C:\WINDOWS\csrss.exe
Avira AntiVir CE 7.0	+	Переименован и удален после перезагрузки C:\WINDOWS\csrss.exe
AVZ 4.21	+	Удален %WINDOWS%\System32\drivers\SYSpnch.sys и %WINDOWS%\csrss.exe
BitDefender Antivirus 10	+	При перезагрузке удален C:\WINDOWS\csrss.exe
Dr.Web Anti-Virus 4.33	+	При перезагрузке удален C:\WINDOWS\csrss.exe
Eset NOD32 Antivirus 2.7	+	Удален %WINDOWS%\System32\drivers\SYSpnch.sys и %WINDOWS%\csrss.exe
F-Secure Anti-Virus 2007	+	Помещен в карантин и удален %WINDOWS%\csrss.exe
Kaspersky Anti-Virus 6.0	+	При перезагрузке удален C:\WINDOWS\csrss.exe
McAfee VirusScan 2007	+	Детектирован и автоматически удален после перезагрузки C:\WINDOWS\csrss.exe
Panda Antivirus 2007	+	При перезагрузке удален C:\WINDOWS\csrss.exe
Sophos Anti-Virus 6.0	+	Переименован и удален после перезагрузки C:\WINDOWS\csrss.exe
Symantec Norton AntiVirus 2007	+	Автоматически помещен в карантин C:\WINDOWS\csrss.exe
Trend Micro PC-Cillin 2007	+	При перезагрузке удален C:\WINDOWS\csrss.exe
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	Worm.Win32.Feebs
Avast! Professional Edition 4.7	-	Удалил только файл mszt32.dll, не детектирует msdl.exe и msry папке %System%.
AVG Anti-Virus PE 7.5	-	Детектируется только родительский файл.
Avira AntiVir CE 7.0	+	Находит и удаляет файлы msdl.exe, msry, mszt32.dll (после переименования и перезагрузки) в папке %System%.
AVZ 4.21	-	Не удается запустить антивирус.
BitDefender Antivirus 10	+	Находит и удаляет файлы msdl.exe, msry, mszt32.dll (после переименования и перезагрузки) в папке %System%.
Dr.Web Anti-Virus 4.33	-	Не удается установить антивирус, зависание на половине установки (компонента Spyder Mail).
Eset NOD32 Antivirus 2.7	+	Находит и удаляет файлы msdl.exe, msry, mszt32.dll (после перезагрузки) в папке %System%.
F-Secure Anti-Virus 2007	+	Находит и удаляет файлы msdl.exe, msry, mszt32.dll (после переименования и перезагрузки) в папке %System%.
Kaspersky Anti-Virus 6.0	-	Не удается установить антивирус, запуск мастера настройки блокируется.
McAfee VirusScan 2007	+	Находит и удаляет файлы msdl.exe, mszt32.dll (после перезагрузки) в папке %System%. Не находит файл msry.
Panda Antivirus 2007	-	Вредоносная программа не обнаруживается (детектируется только родительский файл). Работа антивируса нарушается (процесс Generis Host Process аварийно завершается,
Sophos Anti-Virus 6.0	+	Находит и удаляет файлы msdl.exe, msry, mszt32.dll (после перезагрузки) в папке %System%.
Symantec Norton AntiVirus 2007	+	Находит и удаляет файлы msdl.exe, msry, mszt32.dll (после перезагрузки) в папке %System%.
Trend Micro PC-Cillin 2007	-	Детектируется только родительский файл.
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/

Антивирус	Вердикт	Trojan-Clicker.Win32.Costrat
Avast! Professional Edition 4.7	-	Детектируется только родительский файл.
AVG Anti-Virus PE 7.5	-	
Avira AntiVir CE 7.0	-	
AVZ 4.21	+	Находит RootKit pe386 C:\WINDOWS\system32:lzx32.sys и и удаляет.
BitDefender Antivirus 10	-	Детектируется только родительский файл.
Dr.Web Anti-Virus 4.33	-	
Eset NOD32 Antivirus 2.7	-	
F-Secure Anti-Virus 2007	-	
Kaspersky Anti-Virus 6.0	-	
McAfee VirusScan 2007	-	
Panda Antivirus 2007	-	
Sophos Anti-Virus 6.0	-	
Symantec Norton AntiVirus 2007	+	Обнаружен и удален после перезагрузки %System%:lzx32.sys
Trend Micro PC-Cillin 2007	-	Детектируется только родительский файл.
VBA32 Antivirus 3.11	-	

http://www.anti-malware.ru/

Антивирус	Вердикт	Trojan-Spy.Win32.Goldun
Avast! Professional Edition 4.7	+	Успешно детектирует и удаляет файлы CsdDriver.sys и MemMan.dll (после перезагрузки) в папке %System%.
AVG Anti-Virus PE 7.5	+	Успешно детектирует и удаляет файлы CsdDriver.sys и MemMan.dll в папке %System%, а также MemMan.dllh и Asd19B.tmp.exe
Avira AntiVir CE 7.0	-	После установки обнаруживает %System%\CsdDriver.sys, но не может удалить/переименовать или поместить в карантин (file could not be accessed).
AVZ 4.21	-	Не обнаруживает признаков заражения.
BitDefender Antivirus 10	-	После установки обнаруживает только %System%\CsdDriver.sys, который появляется снова, MemMan.dll детектирует при загрузке, но не может удалить.
Dr.Web Anti-Virus 4.33	-	После установки и экспресс-проверки находит %System%\CsdDriver.sys, после перезагрузки машина постоянно зависает.
Eset NOD32 Antivirus 2.7	+	Успешно детектирует и удаляет файлы %System%\CsdDriver.sys и MemMan.dll (после перезагрузки) в папке %System%.
F-Secure Anti-Virus 2007	-	После установки обнаруживает %System%\CsdDriver.sys, но не может удалить/переименовать или поместить в карантин.
Kaspersky Anti-Virus 6.0	-	После установки антивирус не запускается.
McAfee VirusScan 2007	-	Детектируется только родительский файл.
Panda Antivirus 2007	-	Детектируется только родительский файл.
Sophos Anti-Virus 6.0	+	После перезугрузки успешно детектирует и удаляет файлы %System%\CsdDriver.sys и MemMan.dll в папке %System%.
Symantec Norton AntiVirus 2007	+	После перезугрузки успешно детектирует и удаляет файлы %System%\CsdDriver.sys и MemMan.dll в папке %System%.
Trend Micro PC-Cillin 2007	-	Детектирует файл MemMan.dll в папке %System%, но удалить автоматически не может, предлагает сделать это вручную.
VBA32 Antivirus 3.11	-	Не может открыть для проверки зараженных dll.

http://www.anti-malware.ru/